

On page 8 line 13, after "global server", delete "of".

On page 10 line 6, after "protected by a" please delete "global".

On page 10 line 6, after "firewall 104", insert (referred to herein as a "global
firewall" 104)--.

On page 13 line 10, before "applets", delete "Download" and insert therefor --
Downloaded--.

On page 15 line 8, after "whether", delete "the" and insert therefor --a--.

On page 15 line 14, after "a web", delete "engine" and insert therefor --server--.

On page 15 line 20, after "web", delete "engine" and insert therefor --server--.

On page 16 line 1, after "web", delete "engine" and insert therefor --server--.

On page 16 line 1, after "host engine", delete "286" and insert therefor --386--.

On page 19 line 6, delete the hyphen between "previously" and "generated".

On page 20 line 3, after "the web", delete "page".

On page 20 line 4, before "387", delete "engine" and replace therefor --server--.

On page 22 line 9, after "(SSL)", delete "technology".

IN THE DRAWINGS:

In FIG. 3, please change element 387 from "Web Engine" to --Web Server--.

IN THE CLAIMS:

(Unamended claims are being provided for the convenience of the Examiner.)

- ~~Sub~~
~~BT~~
1. (Once amended) A system comprising:
a communications engine for establishing a communications link with a client;
security [means] services coupled to the communications engine for determining
client privileges;

a servlet host engine coupled to the security [means] services for providing to the client, based on the client privileges, an applet which enables I/O with a [secured] service; and

a key safe for storing a key [which enables] for establishing a connection with [access to] the [secured] service.

2. (Once amended) The system of claim 1, wherein the communications engine uses SSL [technology] to create a secure communications link with the client.

3. The system of claim 1, wherein communications engine negotiates an encryption protocol for transferring messages to and from the client.

4. The system of claim 1, wherein the communications engine uses public key certificates for transferring messages to and from the client.

5. (Once amended) The system of claim 1, wherein the security [means] services use[s] public key certificates to authenticate the client.

6. (Once amended) The system of claim 1, wherein the security [means] services examine[s] client identity and the level of authentication to determine client privileges.

7. (Once amended) The system of claim 1, wherein the security [means] services examine[s] a [global] public key certificate to authenticate the client.

8. (Once amended) The system of claim 1, wherein the security [means] services use[s] digital signature [technology] to authenticate the client.

9. (Once amended) The system of claim 1, wherein the servlet host engine forwards to the client a security applet for enabling the client to perform a security protocol recognized by the security [means] services.

10. (Once amended) The system of claim 1, wherein the service is secured by a [corporate] firewall and the key is configured to enable communication through the firewall.
11. (Once amended) The system of claim 1, further comprising a [global] firewall for protecting the system.
12. (Once amended) The system of claim 1, [further comprising a service] wherein the key includes an address [for] identifying the location of the [secured] service.
13. (Once amended) The system of claim 1, wherein the applet provides to the client a direct connection with the [secured] service.
14. (Once amended) The system of claim 1, further comprising a proxy in communication with the [secured] service, and wherein the applet enables I/O with the proxy and the key enables the proxy to locate the service.
15. (Once amended) A method comprising the steps of:
establishing a communications link with a client;
determining client privileges;
providing to the client, based on the client privileges, an applet which enables I/O with a [secured] service; and
retrieving a key for establishing a connection with [which enables access to] the [secured] service.
16. (Once amended) The method of claim 15, wherein establishing a communications link includes the step of using SSL [technology] to create a secure communications link with the client.

17. The method of claim 15, wherein establishing a communications link includes the step of negotiating an encryption protocol for transferring messages to and from the client.

18. The method of claim 15, wherein establishing a communications link includes the step of using public key certificates for transferring messages to and from the client.

19. The method of claim 15, wherein determining client privileges includes the step of using public key certificates to authenticate the client.

20. The method of claim 15, wherein determining client privileges includes the step of examining client identity and the level of authentication to determine client privileges.

21. (Once amended) The method of claim 15, wherein determining client privileges includes the step of examining a [global] public key certificate to authenticate the client.

22. (Once amended) The method of claim 15, wherein determining client privileges includes the step of using a digital signature [technology] to authenticate the client.

23. The method of claim 15, wherein establishing a communications link includes forwarding to the client a security applet for enabling the client to perform a recognized security protocol.

24. (Once amended) The method of claim 15, further comprising the step of using the key to communicate through a firewall to the [secured] service.

25. (Once amended) The method of claim 15, wherein the method is performed by a [global] server and further comprising using a [global] firewall to protect the [global] server.

26. (Once amended) The method of claim 15, [further comprising using a service] wherein the key includes an address [to identify] identifying the location of the [secured] service.

27. (Once amended) The method of claim 15, wherein providing includes the step of providing to the client a direct connection with the [secured] service.

28. (Once amended) The method of claim 15, further comprising using a proxy in communication with the [secured] service, and wherein providing includes enabling I/O with the proxy.

A3
29. (Once amended) A system comprising:
means for establishing a communications link with a client;
means for determining client privileges;
means for providing to the client, based on the client privileges, an applet which enables I/O with a secured service; and
means for retrieving a key for establishing a connection with [which enables access to] the [secured] service.

30. (Once amended) A computer-based storage medium storing a program for causing a computer to perform the steps of:
establishing a communications link with a client;
determining client privileges;
providing to the client, based on the client privileges, an applet which enables I/O with a [secured] service; and
retrieving a key [which enables access to] for establishing a connection with the [secured] service.